DOCKET FILE COPY ORIGINAL

BEFORE THE

FEDERAL COMMUNICATIONS COMMISSION

WASHINGTON, D.C. 20554

In the Matter of

Amendment of Parts 2, 15, 18 and Other	)	
Parts of the Commission's Rules to Simplify	)	ET Docket No. 97-94
and Streamline the Equipment Authorization	)	
Process for Radio Frequency Equipment	)	

REPLY COMMENTS OF NEXTLEVEL SYSTEMS, INC.

NextLevel Systems, Inc.[1], respectfully submits these reply comments on the Notice of Proposed Rulemaking in the above-captioned proceeding.[2]

NextLevel supports the Commission's proposal to change the equipment authorization process for "cable system terminal devices" ("CSTDs") from notification to certification "to ensure against the marketing of such devices for theft of cable service,"[3] but opposes several additional proposals contained in comments submitted in this proceeding.

---

[1] Created in the strategic restructuring of General Instrument Corporation on July 28, 1997, NextLevel Systems, Inc., is a leading world supplier of high-performance network systems delivering video, voice, and Internet / data services to the cable, MMDS, telephony and satellite markets.

[2] In the Matter of Amendment of Parts 2, 15, 18 and Other Parts of the Commission's Rules to Simplify and Streamline the Equipment Authorization Process for Radio Frequency Equipment, ET Docket No. 97-94, FCC 97-84, released March 27, 1997 ("Notice").

[3] Notice at ¶ 16.

The proposed change to certification illustrates the Commission's recognition that multichannel video service providers ("MVPDs") are fighting a tremendous battle against pirate box manufacturers and others who attempt to defeat CSTD access control systems in order to steal programming. NextLevel has combatted piracy from the beginning of its business as a terminal device manufacturer. Recently, NextLevel's efforts were highlighted on the front page of the *Wall Street Journal*.[4] As the final paragraph of the article suggests, pirate boxes have become so valuable that their manufacture and distribution is now believed connected to organized crime.

Time Warner, in their comments in this proceeding, accurately describe the continuous focus that service providers and legitimate manufacturers must give to the increasingly sophisticated black market for video theft devices. It would be very harmful to the industry for pirate box manufacturers to be able to obtain FCC equipment authorization. Government authorization would provide an air of legitimacy to these illegal products and would make court proceedings against pirates more difficult to pursue.

The Commission's proceeding to implement commercial availability of "navigation devices" makes the outcome of this proceeding even more crucial[5]. Again, as Time Warner points out in its comments, "manufacturers and/or distributors of unauthorized decoders have raised as a defense the argument that Section 629 [added by

---

[4] Mark Robichaux, "Cable Pirates Sought Plunder but Blundered Into a Major FBI Sting," Wall Street Journal, May 12, 1997, at A1.

[5] In the Matter of Implementation of Section 304 of the Telecommunications Act of 1996, Commercial Availability of Navigation Devices, Notice of Proposed Rulemaking, CS Docket No. 97-80, FCC 97-53, released February 20, 1997.

Section 304 of the Telecommunications Act of 1996] establishes a federal right for consumers to purchase and own their own equipment – even pirate boxes used to aid in theft of service."[6] As terminal devices become available through distribution outlets not under the control of the cable operator, such as retail outlets and direct distributors, it becomes even more imperative that the equipment authorization process enable the Commission staff to deter and detect applications involving pirate boxes.

However, it is equally imperative that any changes to the Commission's equipment authorization process not create undue burdens on legitimate manufacturers. This is, unfortunately and unintentionally, the case with several suggestions made by Time Warner in this proceeding. Such burdens will harm not only legitimate manufacturers, but the cable, satellite and wireless operators that these manufacturers supply. In the end, of course, the consumer is harmed by delays in new services or by increased costs in the lease or purchase of equipment.

1. NextLevel Systems supports the Commission's proposed change from notification to certification for cable system terminal devices.

NextLevel supports the Commission's proposal to "[r]elax the requirements from certification or notification to the DoC procedure for the following Part 15 unintentional radiators: CB receivers, superregenerative receivers; all other Part 15 receivers; and, TV Interface Devices (including video cassette recorders and TV video games), except that [the Commission] will require certification for cable system terminal devices to ensure

[6] Comments of Time Warner Cable at 6.

against marketing of such devices for theft of cable service."[7] The relaxation of the regulatory burden on the other Part 15 devices is welcome, while the increased regulatory burden on CSTDs will not create an undue burden on terminal device manufacturers. It has, in fact, been the practice of the Commission staff to require more technical data from terminal device manufacturers than was called for under the notification procedure. Therefore, the regulatory change is essentially a codification of the existing Commission practice and will not burden legitimate manufacturers.

2. While NextLevel Systems supports Time Warner in the fight against program theft, several of Time Warner's proposals would create too heavy a burden on legitimate manufacturers. Specifically, the call for a 60 day wait for "final" equipment authorization should be rejected, but, in line with Time Warner's reasoning, the equipment authorization process should be changed to require the publication of applications at the time of filing.

First and foremost, NextLevel agrees with the overall theme of Time Warner's comments – that pirate box manufacturers must never be given the apparent stamp of legitimacy that a FCC equipment authorization provides, especially as we move toward commercial availability of MVPD equipment. However, NextLevel must object to several of the proposals made by Time Warner concerning additional processes the Commission could implement to deter or detect pirate box manufacturers. Most important is the suggestion by Time Warner that CSTD authorizations "not become final until 60 days after the public notice of the application grant is published" (emphasis in original).[8] Time Warner suggests this 60 day period be used by interested parties to seek

[7] Notice at ¶ 16.
[8] Comments of Time Warner Cable at 9.

reconsideration of the Commission's grant of authorization or to bring any "irregularities" to the Commission's attention.[9]

This proposal, while well-intentioned, will severely harm legitimate manufacturers. When a piece of equipment is submitted to the Commission for equipment authorization, that device has been through the testing process and is likely already in the beginning of the manufacturing cycle. Once an application is filed, the equipment authorization process generally takes 30 to 40 days. The grant of authorization is the final step needed to complete contracts and start shipping the product. Generally, upon grant of authorization, the first shipments of a product model begin immediately so the customers, in turn, can deliver it to their subscribers.

This two-month delay would be unacceptable to legitimate manufacturers and to the majority of their cable and satellite customers. For operators to be competitive in offering new services, they must first provide their subscribers with the equipment to receive those services. As the industry continues its transition to digital, the technology involved in delivering multichannel video and data services to subscribers is undergoing a period of rapid technological innovation. This means a constant influx of new models with new features, some of which will have only a short product life cycle before being replaced by an improved technology. Operators already wait for new products to be developed, to be tested in the laboratory, to be tested in the field, and finally, to receive equipment authorization. An additional two month wait delays the delivery of innovative

[9] Id.

products to consumers and harms the ability of operators to compete via new service offerings.

However, while NextLevel objects to the specific suggestion of a 60 day period before finalization of equipment authorization, NextLevel agrees with Time Warner that the process requires change. Currently, applications are made public when the equipment authorization is granted. As Time Warner's suggestion illustrates, this is when industry participants finally can discover any "irregularities" identifying a possible pirate manufacturer. If the authorization process were changed to allow publication of the application at the time of filing, Time Warner's call for a comment period for interested parties would be fulfilled. Not only would Commission staff examine an application for legitimacy, but cable operators and legitimate manufacturers would have an opportunity to bring any irregularities or suspicious statements to the attention of the Commission. The added value of such an approach is that pirates would be brought to Commission attention before a grant of equipment authorization, obviating the need to delay "final" authorization for any amount of time or to revoke an authorization. The purpose behind Time Warner's suggested 60 day wait is to provide industry participants with input on the equipment authorization process to help detect applications for illegal boxes; publishing equipment authorization applications when they are filed would satisfy that purpose, and not harm legitimate manufacturers.

3. Time Warner also proposes that the Commission (1) adopt a standard to prevent the manufacture of terminal devices which allow easy deactivation or bypass of access control features and (2) require applicants to provide a description of access control features. While these proposals may help detect pirates, to the extent that they might be

read by the Commission as a call for the adoption of a security standard or would require filings which detail access control systems, they should be rejected by the Commission.

A second suggestion by Time Warner is that the Commission "adopt a standard that prevents unscrupulous companies from manufacturing substandard terminal equipment which allows the conditional access or scrambling/encryption functions to be easily deactivated or bypassed."[10] To the extent that the Commission understands this to be a call for adoption of an encryption or security standard for cable system terminal devices, NextLevel urges the Commission not to adopt the proposal. NextLevel does not believe this was the intended meaning of Time Warner.

The Commission has faced this subject on several prior occasions and has always correctly declined to take action on a security standard. In 1989, the Commission, under instruction of Congress, undertook an inquiry into the need for a universal encryption standard for satellite cable programming.[11] The Commission concluded that a mandatory encryption standard was unnecessary, would involve a protracted proceeding, would diminish industry incentives to combat piracy, and could compromise the integrity of the standard adopted.[12] While the MVPD industry has changed significantly since 1989, these findings remain valid.

The security standard issue recently reappeared in the retail sale proceeding, where Congress declared that any rules adopted by the Commission must be done in consultation with industry standard-setting efforts and must not harm the security of

---

[10] Id.

[11] See, In the Matter of Inquiry into the Need for A Universal Encryption Standard for Satellite Cable Programming, Report, GEN Docket No. 89-78, FCC 90-142, released April 25, 1990.

[12] Id. at ¶¶ 69-71.

operators' networks. The vast majority of commenters in that proceeding urged the Commission to avoid mandating standards. NextLevel urges the Commission, once again, to realize that a security standard merely enables pirates to focus their collective time and energy toward defeating one system. In addition, manufacturers lose the incentive to research and develop new techniques for network security, stifling innovation. The Commission must continue to reject any perceived calls for security standards.

In a related suggestion, Time Warner asks that the Commission require CSTD equipment authorization applicants "to provide a detailed description of the features contained in the equipment for which approval is sought which are designed to prevent unauthorized access to programming, and to prevent unlawful modification of the equipment."[13] Again, depending on how the Commission reads this proposal, it could place an undue burden on legitimate manufacturers of cable system terminal devices.

Time Warner does not elaborate as to what "a detailed description" of security features would entail, but its suggestion likely addresses the fact that the Commission currently asks equipment authorization applicants only if their equipment is "addressable"; no further elaboration is required. Pirate boxes contain much of the same circuitry and functionalities as contained in legitimate terminal devices. Thus, a pirate can answer that its box is addressable, yet does not have to mention that the box will not accept the access control commands of any current cable operators' access control

[13] Comments of Time Warner Cable at 9.

computer. Some elaboration in this portion of the equipment application would help detect pirate manufacturers without harming legitimate manufacturers.

However, to the extent that the Commission reads Time Warner's suggestion as requiring a detailed description of access control features, such as disclosing proprietary information involving the algorithms and other security mechanisms used, the proposal should be rejected. The scrambling and access control systems involved are at the heart of the war against piracy. Companies such as NextLevel work very hard to stay one step ahead of the pirates by guarding security information and by researching and developing new tools to combat signal theft. These realities point up one of the reasons that the very idea of standardization is antithetical to the concept of security: standardization implies public disclosure; security requires maintaining secrets.[14]

4. NextLevel Systems supports the further proposals of Time Warner, especially the idea of an expedited revocation of equipment authorization when equipment is determined to have been intended for the piracy of cable programming.

Time Warner makes three additional suggested changes to the equipment authorization rules to help deter piracy: (1) that applicants must detail steps taken to ensure that the equipment is going only to legitimate cable equipment distributors, (2) that the Commission adopt a presumption that entities shown to have engaged in pirate activities within the past 10 years may not receive equipment authorization, and (3) that

[14] An even more difficult question would be raised by any requirement of disclosure of proprietary information. We question the Commission's authority to adopt such a requirement. We believe that it would not be consistent with sound public policy and would be contrary to the Commission's sound practices.

an expedited revocation procedure be instituted to strip authorization from those who have received it and then engaged in piracy activities.[15]

NextLevel generally supports these ideas as beneficial to the authorization process and not overly burdensome on legitimate manufacturers. At the time of filing an application for authorization, a legitimate manufacturer cannot know all the possible customers for a particular product over the lifetime of the product, but the manufacturer would certainly be able to list those customers, including system operators, retail outlets or direct distributors, with which it has a conditional contract or letter of intent. The Commission, however, should respect any requests by manufacturers to keep such information confidential.

NextLevel also supports a presumption against granting equipment authorizations to parties known to be pirate manufacturers or to be linked to pirate activities. Pirate manufacturers will create different models of equipment and will continue to apply for equipment authorization following prior unsuccessful attempts to receive such authorization. They do not have a history of dropping out of the business after getting caught. Most pirates simply create a new company and try again.

Lastly, NextLevel strongly supports the concept of an expedited revocation procedure. The idea of speedily revoking the authorization on equipment proven to have been intended for the theft of multichannel video service is beneficial to the industry as a whole. The Commission should continue to devote the majority of its resources in this area to seeing that equipment authorizations are not granted to pirate manufacturers in the

[15] Id. at 9-10.

first place; so far, most pirates have been unable to successfully sneak their product by the Commission staff. But while prevention is the best method for fighting authorization of pirate equipment, revocation of wrongfully obtained authorizations certainly will aid the battle.

When a piece of equipment is given authorization and later discovered to be a pirate device, it is important that the equipment not continue to carry the label of "authorized." This is especially true given the value the courts have placed on equipment authorization during the trials of pirate manufacturers. A quick revocation process would help ensure that by the time the case went to court, the pirate manufacturer could not rely on a valid government equipment authorization as part of its defense.

5. NextLevel Systems, while supporting the Commission's proposed change from notification to certification for cable system terminal devices, suggests the adoption of a more equitable fee schedule for certification applicants.

NextLevel objects to the proposed change in the fee schedule for cable system terminal device applications. Under notification, NextLevel and others were required to pay a fee of $140 per application. The Commission proposes that "under the new combined certification procedure the fee will be $895 for devices operating under Parts 15 and 18 of the rules and $450 for everything else."[16] NextLevel objects to the more than six-fold increase in application fee for cable system terminal devices. This increase burdens legitimate manufacturers who design and construct many different models of their products, for digital and analog, for cable and satellite, and who always seek FCC

[16] Notice at ¶ 14.

authorization for their equipment. Applicants for CSTD equipment authorization already submit the same data that will be required for submittal under the proposed rules; no additional work will be imposed on Commission staff. Thus, there appears to be no justification for the six-fold increase.

NextLevel proposes that the Commission adopt a flat fee of $450 for all equipment subject to certification. The Commission states in the Notice that type acceptance and certification were very similar processes.[17] The same amount of technical data and information will be required for all equipment now needing certification and the staff attention required by Part 15 and Part 18 equipment applications will in most cases equate that of equipment used in authorized radio services. With a flat certification fee of $450, all equipment and manufacturers subject to certification will be treated equally, while the equipment authorization process will be further simplified.

6. NextLevel Systems urges the Commission not to adopt a "voucher" system for obtaining sample equipment from the market. NextLevel supports Motorola and the Information Technology Industry Council in their alternative proposals to the Commission.

In its Notice of Proposed Rulemaking, the Commission also addresses its need to improve oversight of the compliance of equipment on the market. The Commission proposes that when it requests a sample of a product for testing, and that product is widely available on the retail market, the manufacturer will provide the Commission staff with a "voucher" so that the staff may purchase a sample product directly from a retail

[17] Id. at ¶ 6.

outlet.[18] Both Motorola and the Information Technology Industry Council objected to this proposed process as needlessly complex.[19] NextLevel agrees.

Some MVPD equipment is already being sold at retail, while the market is driving other equipment, including terminal devices, toward retail distribution. The idea of a "voucher" system to obtain samples of such equipment does indeed seem needlessly complicated. The Commission's proposal appears to involve some form of "coupon" that manufacturers would have to create and supply to the Commission staff. Those staff members would then present the coupon to the cashier of a retail outlet and take the product for free; the manufacturer would reimburse the retailer. What such a coupon would look like and how the system would work would all need to be addressed; however, some form of bureaucratic system would appear to be the end result. As Motorola pointed out in its comments, such a system also would appear to invite fraud.[20] In addition to a pirate box market, we would have a pirate coupon market for people attempting to obtain free equipment.

Motorola suggests that Commission staff simply purchase the equipment at retail and seek reimbursement from the manufacturer.[21] ITI suggests that the manufacturer be required to provide the Commission with a sample product taken directly from the retail distribution chain and unaltered.[22] Either of these suggestions appears to be less

[18] Id. at ¶ 15.
[19] See Comments of Motorola at 12-13 and Comments of the Information Technology Industry Council ("ITI") at 8.
[20] See Comments of Motorola at 13.
[21] Id.
[22] See comments of ITI at 8.

burdensome and inherently less open to fraud than the Commission's proposal for a voucher system. NextLevel supports Motorola and ITI in their alternative proposals.

CONCLUSION

In this proceeding, and indeed in the work of the Commission staff in carrying out the equipment authorization process, the Commission has actively shown its recognition of the piracy problem which plagues the multichannel video industry. It is essential that pirate manufacturers never receive FCC authorization – such an air of legitimacy would only exacerbate a $5 billion a year theft of service problem.[23] But it is equally important that legitimate manufacturers, whose products will continue to bring new and innovative services to millions of paying subscribers, not be unduly burdened in the quest to capture

[23] 1995 NCTA Theft of Service Survey, reported April 7, 1997.

the thieves. For this reason, NextLevel urges the Commission to adopt only those limited changes to its equipment authorization process that will work to deter and detect pirate manufacturers without harming legitimate manufacturers.

Respectfully submitted,

NextLevel Systems, Inc.

Quincy Rodgers,
Vice President, Government Affairs
Christine G. Crafton,
Director, Industry Affairs
Faye R. Morrison,
Government Affairs Representative

NextLevel Systems, Inc.
Two Lafayette Centre
1133 21st Street, NW, Suite 405
Washington, DC 20036
(202) 833-9700

August 18, 1997